Effect of Device Imperfection on Reference Frame Independent Quantum Key Distribution

Kyongchun Lim, Byung-Seok Choi, Ju Hee Baek, Minchul Kim, Joong-Seon Choe, Kap-Joong Kim, Young-Ho Ko, Chun Ju Youn

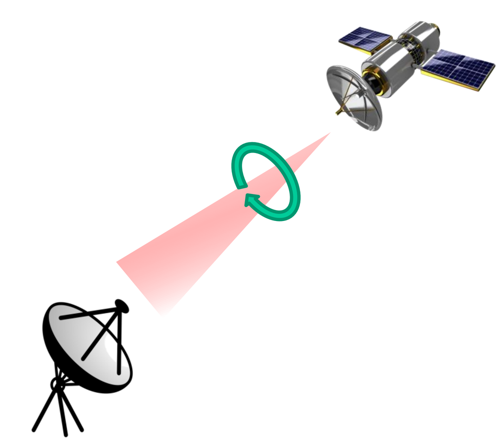
Electronics and Telecommunications Research Institute (ETRI), Daejeon, 34129, KOREA

Free-Space Quantum Key Distribution (QKD)

- **A promising solution for secure communication between two remote parties through free space**
  - No requirement of physical connection between two remote parties
  - Applicable to moving terminals with the characteristics such as moving position, outside operation, and limited internal space

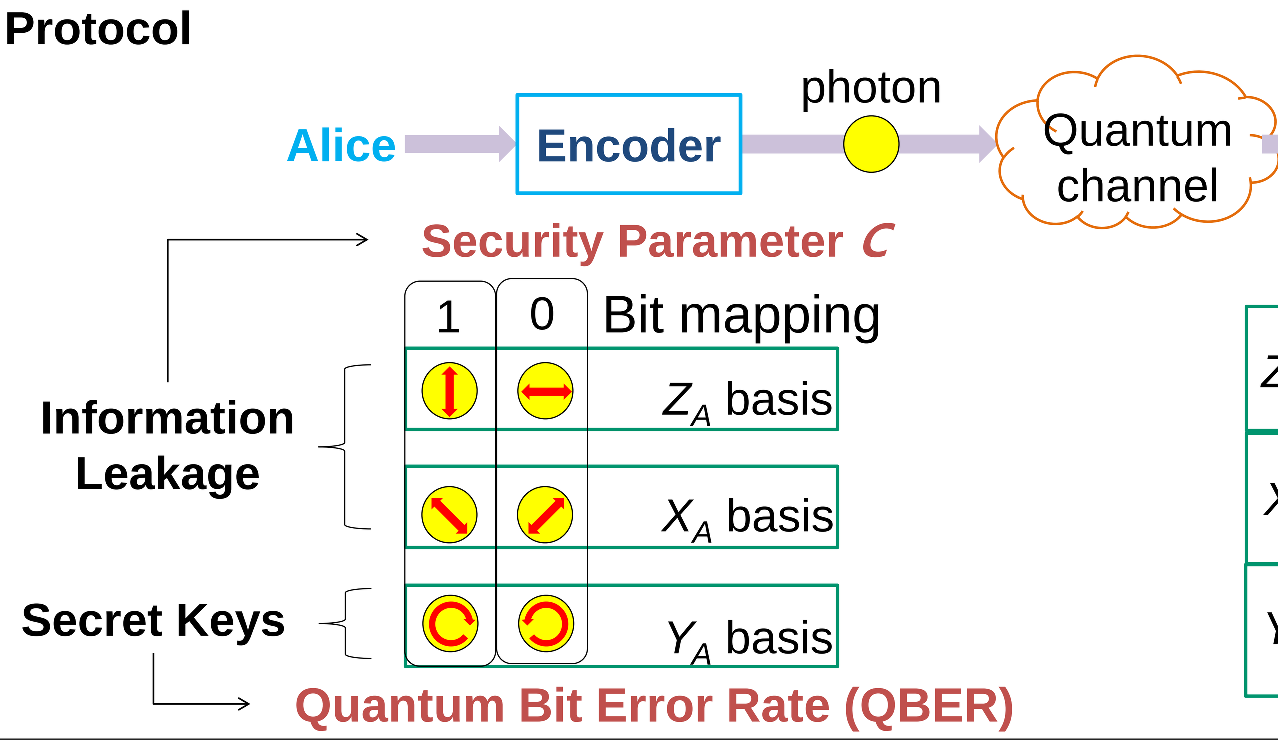
Reference Frame Independent (RFI) Quantum Key Distribution

- **Problem in conventional BB84 protocol**
  - **Reference frame mismatch due to moving terminals**
  - **Increasing QBER and lowering secret key rate**
  - **Real time polarization compensation**



- **Reference frame independent quantum key distribution**
  - **Variant of six-state protocol**
  - **Unnecessary real time polarization compensation**
  - **Secret keys from circular polarization states**
  - **Information leakage from the combination of the linear polarizations**

- **Protocol**



Z_B basis +	Polarization beam splitter
X_B basis ×	Wave plate + Polarization beam splitter
Y_B basis	Wave plate + Polarization beam splitter

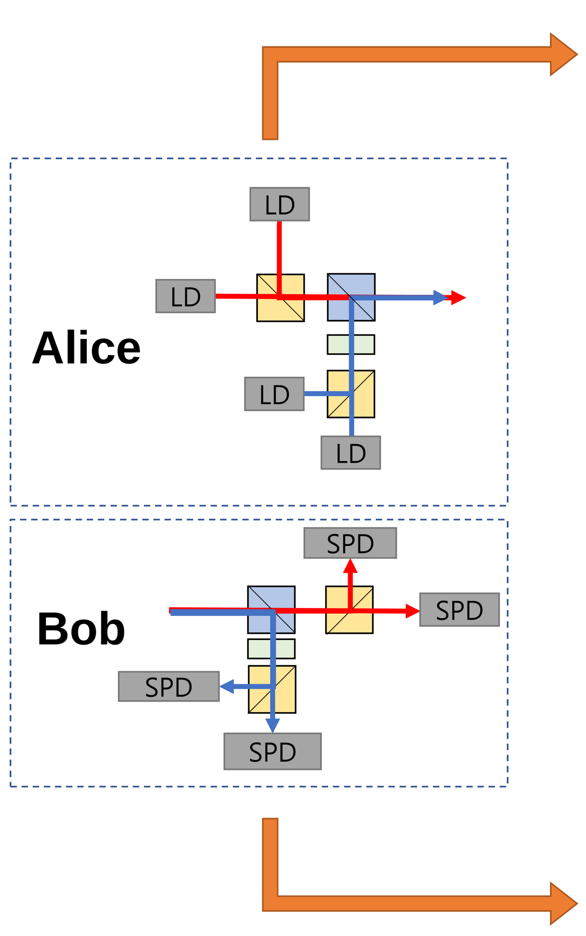
$$C_{ij} = \frac{n_{ij,00} - n_{ij,01} - n_{ij,10} + n_{ij,11}}{n_{ij,00} + n_{ij,01} + n_{ij,10} + n_{ij,11}}$$

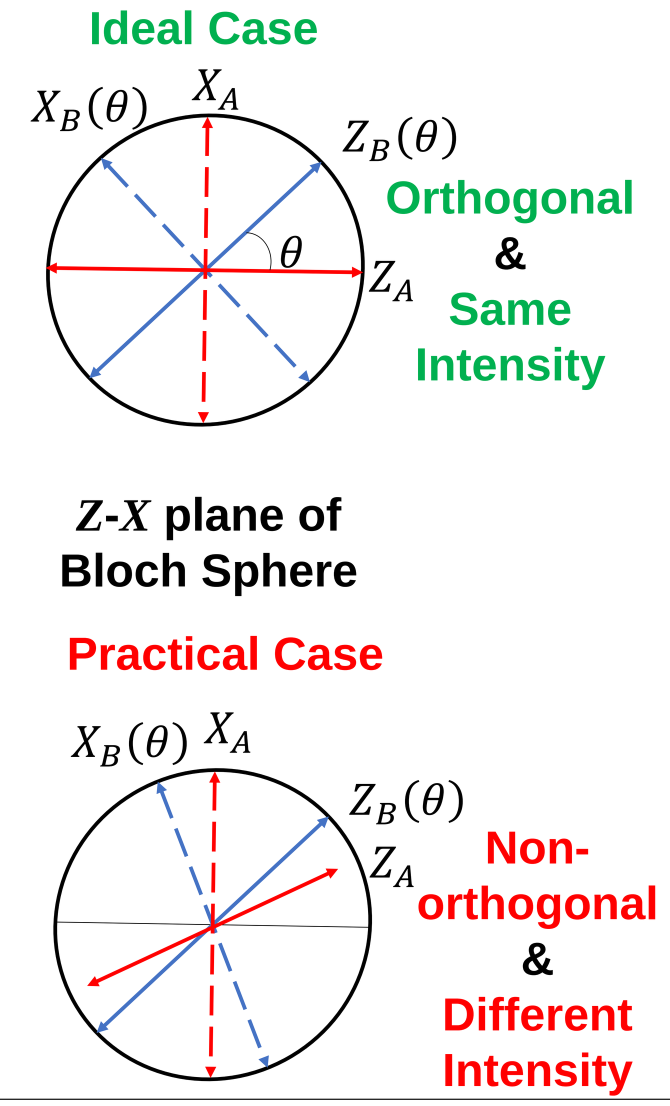
$n_{ij,kl}$ refers to the number of detections when Alice transmits k state in i basis and Bob detects l state in j basis

$$\begin{aligned} C &= C^2_{Z_A Z_B} + C^2_{Z_A X_B} + C^2_{X_A Z_B} + C^2_{X_A X_B} \\ &= C^2_{Z_A(\cos\theta Z_A + \sin\theta X_A)} + C^2_{Z_A(\cos\theta X_A - \sin\theta Z_A)} \\ &+ C^2_{X_A(\cos\theta Z_A + \sin\theta X_A)} + C^2_{X_A(\cos\theta X_A - \sin\theta Z_A)} \end{aligned}$$

$$\text{QBER} = \frac{1 - C_{Y_A Y_B}}{2}$$

Effect of Device Imperfection on Reference Frame Independent Quantum Key Distribution

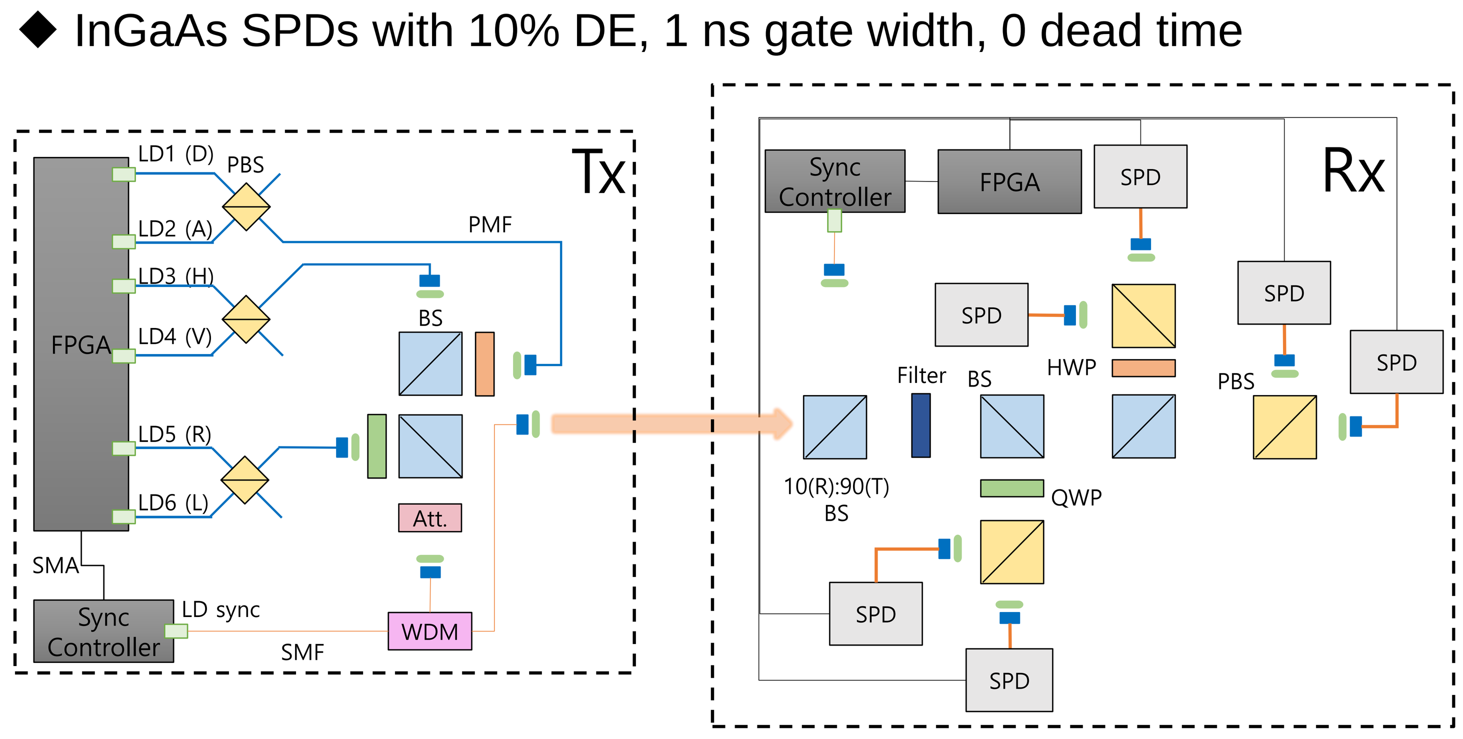


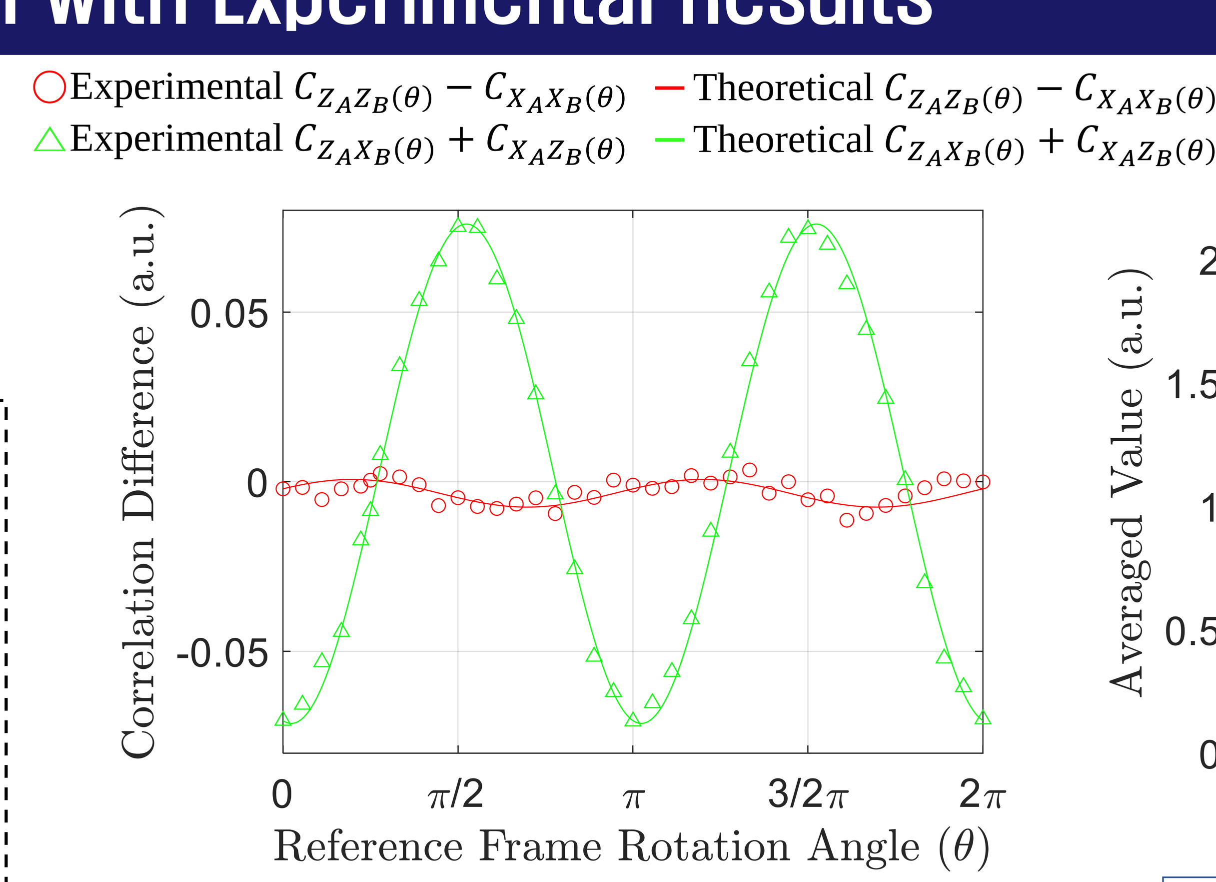


	Ideal Case	Practical Case
Bases	$Z_A = \sigma_Z$ $X_A = \sigma_X$ $Z_B(\theta) = \cos 2\theta\sigma_Z - \sin 2\theta\sigma_X$ $X_B(\theta) = \sin 2\theta\sigma_Z + \cos 2\theta\sigma_X$	$Z_A = (\cos 2\theta_1\sigma_Z - \sin 2\theta_1\sigma_X)\boxed{\cos 2\phi_1 + \sin 2\phi_1\sigma_Y}$ $X_A = (\cos 2\theta_2\sigma_Z - \sin 2\theta_2\sigma_X)\boxed{\cos 2\phi_2 + \sin 2\phi_2\sigma_Y}$ $Z_B(\theta) = (\cos 2(\theta_3+\theta)\sigma_Z - \sin 2(\theta_3+\theta)\sigma_X)\boxed{\cos 2\phi_3 + \sin 2\phi_3\sigma_Y}$ $X_B(\theta) = (\cos 2(\theta_4+\theta)\sigma_Z - \sin 2(\theta_4+\theta)\sigma_X)\boxed{\cos 2\phi_4 + \sin 2\phi_4\sigma_Y}$ Circular Polarization component
Correlations	Symmetric Correlation $C_{Z_A Z_B(\theta)} = C_{X_A X_B(\theta)}$ $C_{X_A Z_B(\theta)} = -C_{Z_A X_B(\theta)}$	Asymmetric Correlation $C_{Z_A Z_B(\theta)} \neq C_{X_A X_B(\theta)}$ $C_{X_A Z_B(\theta)} \neq -C_{Z_A X_B(\theta)}$
Security Parameter	Invariant Security Parameter $C = C^2_{Z_A Z_B(\theta')} + C^2_{Z_A X_B(\theta')} + C^2_{X_A Z_B(\theta')} + C^2_{X_A X_B(\theta')}$ $= C^2_{Z_A Z_B(\theta)} + C^2_{Z_A X_B(\theta)} + C^2_{X_A Z_B(\theta)} + C^2_{X_A X_B(\theta)}$	Variant Security Parameter $C = C^2_{Z_A Z_B(\theta')} + C^2_{Z_A X_B(\theta')} + C^2_{X_A Z_B(\theta')} + C^2_{X_A X_B(\theta')}$ $\neq C^2_{Z_A Z_B(\theta)} + C^2_{Z_A X_B(\theta)} + C^2_{X_A Z_B(\theta)} + C^2_{X_A X_B(\theta)}$

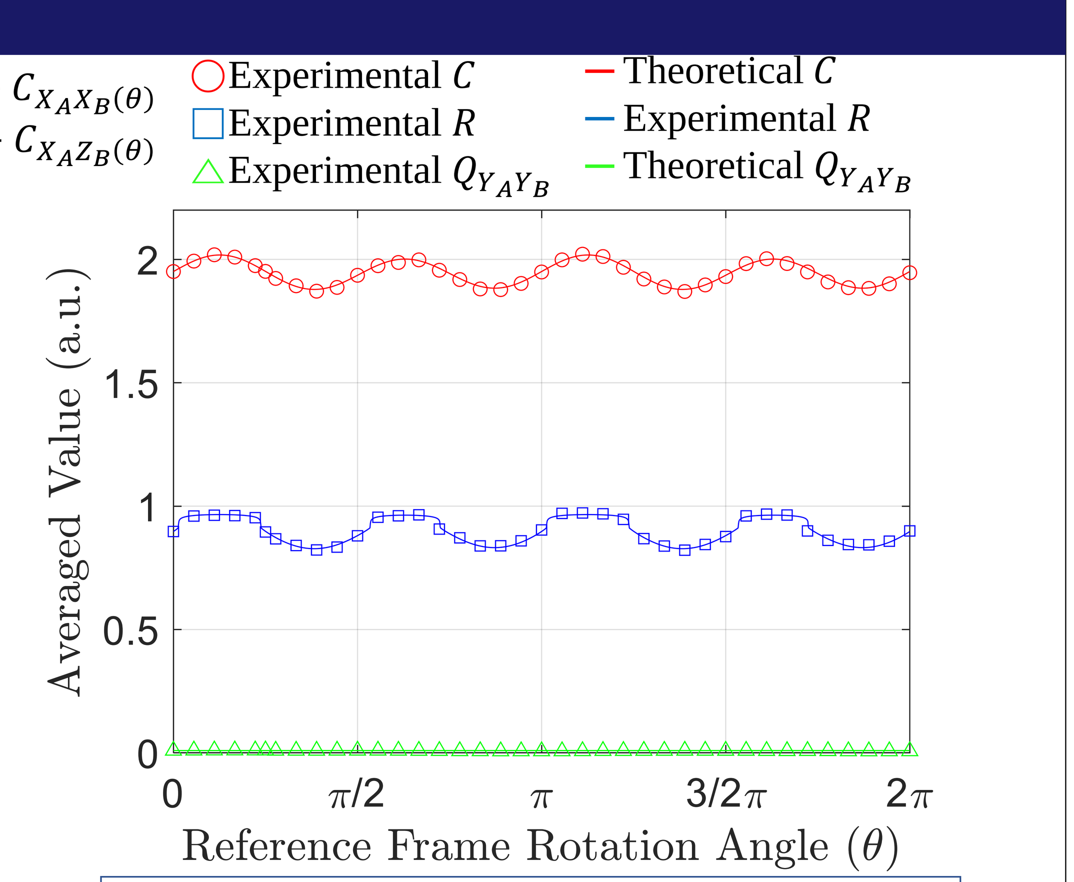
Verification with Experimental Results

- **1550-nm free-space QKD system**
  - 100 MHz repetition rate
  - Fully controlled by FPGA
  - InGaAs SPDs with 10% DE, 1 ns gate width, 0 dead time





Non-zero correlation difference due to asymmetric correlations



Asymmetric correlations causing fluctuation of the security parameter and the corresponding secret key rate R

Conclusion

- **RFI QKD protocol**
  - ✓Independent performance to the varying reference frame
- **Device imperfections in RFI QKD**
  - ✓Asymmetric correlations due to imperfect devices consisting of RFI QKD
  - ✓Reference frame dependent performance

- **Experimental Result**
  - ✓Asymmetric correlation → Fluctuating security parameter → Fluctuating secret key rate

[Reference for more detail]

☞ K. Lim, Optics Express, 29(12)

Electronics and Telecommunications Research Institute